# PCT

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04N 7/167	A1	(11) International Publication Number: WO 00/59225
		(43) International Publication Date: 5 October 2000 (05.10.00)

(21) International Application Number: PCT/US00/04470

(22) International Filing Date: 22 February 2000 (22.02.00)

(30) Priority Data:
09/276,978   26 March 1999 (26.03.99)   US

(71) Applicant: MOTOROLA INC. [US/US]; 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

(72) Inventors: GEIGER, Robert, L.; 1675 Teri Lane, Algonquin, IL 60102 (US). LIN, Jyh–Han; 4931 Northwest 116 Avenue, Coral Springs, FL 33076 (US). MEHTA, Rajiv; 8000 West Sunrise Boulevard, Plantation, FL 33322 (US).

(74) Agents: BOSE, Romi, N. et al.; Motorola Inc., Intellectual Property Dept., 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SECURE WIRELESS ELECTRONIC–COMMERCE SYSTEM WITH WIRELESS NETWORK DOMAIN
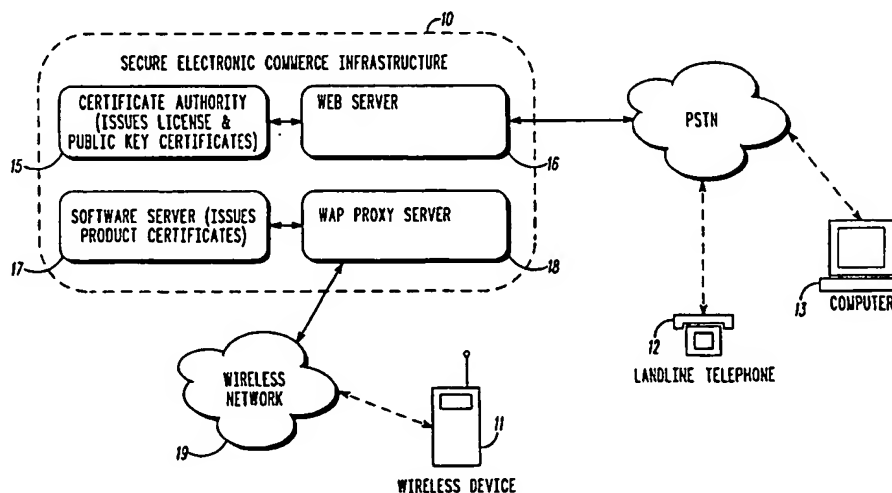
(57) Abstract

A method of conducting transactions in a wireless electronic commerce system, where the system comprises a wireless network operator certification authority (15) having a root public key certificate and at least one attribute authority (404, 405, 406) having a digital certificate that is dependent from the root public key certificate. The attribute authority is accessible by a wireless client device (11) via a wireless network. The digital certificate is delivered from the attribute authority to the wireless device, the attribute authority is verified to the wireless client device using the digital certificate and the root public key certificate preloaded in the wireless client device under authority of the wireless network operator. An attribute (software, service, right/permission or other content item) is delivered to the wireless client device over the wireless network and ultimately enabled at the wireless client device.

SECURE WIRELESS ELECTRONIC-COMMERCE SYSTEM WITH WIRELESS NETWORK DOMAIN

Field of the Invention

5

This invention relates to secure electronic commerce distribution and sales having the ability to offer software enhancements and new features in a simpler, faster, and cheaper method than previously available. Secure electronic commerce brings together three important functions: reprogrammable software or other content (generically referred to also as "product", which includes services); wireless data

10 service; and security (encryption & authentication).

Background of the Invention

15

Secure electronic commerce offers a way for customers to add or change features in their phone using the convenience of the wireless data service already available in the phone. Moreover, the customer can achieve these goals within minutes and in the comfort of the customer's home or business.

Secure electronic commerce offers many advantages, among them: greater

20 ease of distribution, sale and revenue collection for software-only features; flexible and upgradeable phone platform - this reduces obsolescence; ability to thwart theft of services and cloning; reduced warranty costs in case of software patch updates; and convenience of wireless reprogramming.

Summary of the Invention

25

In one aspect, the present invention provides a method of conducting transactions in a wireless electronic commerce system, where the system comprises a wireless network operator certification authority having a root public key certificate

30 and at least one attribute authority having a digital certificate that is dependent from the root public key certificate, where the attribute authority is accessible by a wireless client device via a wireless network. The digital certificate is delivered

from the attribute authority to the wireless device, the attribute authority is verified to the wireless client device using the digital certificate and the root public key certificate pre-loaded in the wireless client device under authority of the wireless network operator. An attribute (software, service, right/permission or other content

5   item) is delivered to the wireless client device over the wireless network and ultimately enabled at the wireless client device.

Payment for the attribute may be transacted by delivering a second digital certificate from the wireless client device to the attribute authority and verifying the second digital certificate using the root public key certificate from the certification

10   authority.

In another aspect, the invention provides a method of conducting transactions in a wireless electronic commerce system that includes establishing a wireless communication between the wireless client device and a first attribute authority; delivering a first attribute to the wireless client device over the wireless network;

15   generating an electronic voucher verifiable by a second attribute authority; establishing a wireless communication between the wireless client device and the second attribute authority; requesting a second attribute from the second attribute authority; identifying the electronic voucher at the second attribute authority; and delivering the second attribute from the second attribute authority to the wireless

20   device.

The electronic voucher may be delivered from the first attribute authority to the second attribute authority via a connection therebetween or may include delivering the electronic voucher from the first attribute authority to the second attribute authority via the wireless client.

25   Also described is a wireless electronic commerce system.

Glossary of Abbreviations

       AA   Attribute Authority

30   API   Application Programming Interface

CA	Certification Authority
DER	Distinguished Encoding Rules (ASN.1)
EC	Elliptic Curve
GSM	Global System for Mobile Communication
ID	Identifier
ME	Mobile Equipment
PER	Packed Encoding Rules (ASN.1)
PIN	Personal Identification Number
PK	Public Key
PKI	Public Key Infrastructure
RA	Registration Authority
RSA	RSA (Rivest, Shamir, Adleman) public key algorithm
SHA-1	Secure Hash Algorithm 1
SIM	Subscriber Identity Module
SMS	Short Message Service
WAP	Wireless Application Protocol
WIM	Wireless Identity Module
WML	Wireless Markup Language
WMLScript	Wireless Markup LanguageScript
WDP	Wireless Datagram Protocol
WTLS	Wireless Transport Layer Security

Brief Description of the Drawings

FIG. 1 is a block diagram of a secure wireless electronic commerce system in accordance with a first aspect of the invention.

FIG. 2 is a flow diagram illustrating software installation and boot-up steps for the wireless client device of FIG.1.

FIG. 3 is a flow diagram illustrating steps in a process of software download to a wireless device in the field or enabling of software in a wireless device in the field.

FIG. 4 is a block diagram of a secure wireless electronic commerce system in
5   accordance with a second aspect of the invention.

FIG. 5 is a flow diagram illustrating steps of operation of the system of FIG. 4.

Detailed Description of the Drawings

10

The overall security model employs cryptographic API and underlying cryptographic toolkits providing a base level of security features, which other stack layers, such as a Wireless Transport Layer Security (WTLS) API, certificate standardization, and wireless applications such as a Wireless Application Protocol
15   (WAP) browser, can build upon. FIG. 1 shows the entities and relationships of the system.

The customer interfaces with the secure electronic commerce system 10 by using a wireless phone 11 or other wireless device plus a landline phone 12 or Internet-accessible computer (dialup, Ethernet, cable, etc.) 13. Various servers 15,
20   16, 17, 18 within the system 10 perform the tasks of secure electronic commerce. Whether directly accessing through an Internet connection 13, or using a conventional telephone 12 to talk with an operator, the customer inputs an order to the secure electronic commerce system 10 at the Web server 16.

The web server 16 communicates with the Certificate Authority server 15 to
25   issue a new Product Certificate. This certificate will ensure that only the targeted phone 11 will be able to obtain and use the new feature. Because the phone originally contained a Product Certificate from the Software Server 17 (while in the factory), an audit trail, or accountability, is maintained for the life of the phone. The phone 11 cannot operate software it was not allowed to based on the content of the

4

certificate. The system 10 also contains a copy of the phone's certificate and so it has a record of the capabilities of the phone.

The Certificate Authority server 15 is a server which creates and distributes Public Key Certificates and License Certificates throughout the secure electronic
5   commerce system.

License Certificates allow devices, such as wireless phones, to operate specified software products. License Certificates are issued to each manufactured device prior to leaving the factory, and subsequently when new software is bought. License Certificates include the device's serial number as part of the data, which
10   when digitally signed by the CA, will bind the right-to-use software license only to the phone that has that serial number, which by design must be unalterable. Therefore, these certificates can only be used by the targeted party and no one else.

Public Key Certificates enable devices to establish trust through the CA. The CA digitally signs the certificate stating that a given device, denoted by its serial
15   number, has the following public key associated with it.

The Web Server 16 is the front-end server for the secure electronic commerce system. It may be a series of servers (i.e. order entry, billing, order processing, etc.) but conceptually is thought of as one entity. This server contains the order entry system by which customers enter orders. Orders may be taken online through the
20   Web, or by phone via an operator. This server completes the order entry by first verifying the user's information (user name, device serial number, credit card, etc.). The Web server then sends a request to the CA for a new License Certificate. The CA sends the License Certificate to the device. The License Certificate may be "pushed" by the CA or sent on-demand from the device. The device now holds the
25   new License Certificate and has been authorized to use the new software.

The Software Server 17 makes available all of the software products sold by the system provider/operator. It may be a series of servers including various factory servers but conceptually is thought of as one entity. The function of the Software Server 17 is to digitally sign software products and make the software product and
30   corresponding certificate (known as the Product Certificate) available for download.

The function of the WAP Proxy Server 18 is to translate HTML syntax into WML syntax (Internet to WAP protocol) and vice-versa.

Certificates are the cornerstone of the secure electronic commerce system and a description of digital certificates can be found in Draft American National Standard

5   X9.68-199x: Digital Certificates for Mobile, Account Based and High Transaction Volume Financial Systems, available from American Bankers Association Standards Department 1120 Connecticut Avenue., NW Washington DC 20036.

Various of the protocols and techniques in the secure electronic commerce system 10 operate on certificates (either reading/parsing certificates, or

10   adding/modifying/deleting certificates). Every device (servers 16, 17 and 18 and wireless devices 11) in the system has one or more certificates. They all have a trusted root certificate which is the Public Key Certificate of the CA from the CA server 15. Given this, the secure electronic commerce system can be deployed.

There now follows a description of the basic certificate types and the use of

15   certificates in the lifetime of a phone.

A Public Key Certificate contains information that ties a wireless device 11 with its public key. This is accomplished by hashing the relevant data. The certificate is comprised of the aforementioned data plus the hash result. Anyone wishing to verify whether the public key belongs to the device only needs to hash the

20   data again, and verify that it matches the hash result stored with the certificate.

Additionally, the hash is digitally signed by a certifying authority. In this model the CA is the trusted certifying authority. That is, the previously mentioned hash result is signed with the CA's private key. Anyone who has the public key for the CA will be able to verify the encrypted hash. Subsequently, if the verified hash

25   result matches that of the user-computed hash of the certificate data, that tells the user that (i) the certificate must have been signed by the trusted CA since the CA's public key was able to properly verify the signed hash and (ii) the certificate does belong to the subject because the subject's private key can verify data signed by the public key.

6

A License Certificate contains information that ties a wireless device 11 with certain access rights. In particular, a License Certificate contains, at a minimum, fields for software product and device serial number. The software product field contains a product identifier. This identifier grants the device a license to use the

5   product. A device will be able to run the specified software product if its internal serial number, embedded in the device, matches the License Certificate's serial number. As in the Public Key Certificate, the data in the License Certificate is hashed and signed by the CA. The device will not be able to verify forged License Certificates since it won't be able to validate the certificate to the CA's signature

10   (unless the CA has been compromised).

A Product Certificate ties a content item or subject (e.g. a software product name) to a fingerprint. In this case, the fingerprint is the hash of the software product. Therefore, anyone who has a software product along with its Product Certificate can verify the integrity of the software by comparing a user-computed

15   hash of the software with the hash result stored in the certificate. As in the Public Key Certificate, the hash result in the Product Certificate is digitally signed by the Motorola CA. So, when the user compares the computed hash with the Product Certificate's hash result, a match implies that the software product is the same which the Motorola CA had digitally signed.

20   Having described the various infrastructure devices and the role that certificates play in the system, the way in which the secure electronic commerce system is deployed can now be described.

The following sections describe briefly how the system functions using examples that occur for a device. The examples chosen are for a phone, and include

25   what happens when the phone is setup in the factory, what happens when a user turns on and uses the phone, and what happens when a user wants to obtain a new feature.

Each phone in the factory has certain some unique characteristics built-in before the unit is shipped. Physically, the phone must contain: (i) ROM available to run unalterable certificate verification code; (ii) EEPROM available to store

30   certificates (access to the certificates storage area must be restricted) and (iii) an

unalterable unique serial number (either in ROM, laser-etched, write-once memory, etc.)

At the factory, a Public Key Certificate is generated for the phone (step 100 of FIG. 2). This can be generated by the Software Server 17, the CA server 15, or by
5   the phone itself. The CA server 15 digitally signs the certificate and retains a copy of it (step 101). The phone is installed with its own Public Key Certificate, plus the CA's Public Key Certificate (102). (The CA, being the root certifying authority, signs its own certificate.) A key assumption is that inside the factory there is a trusted network. In this environment, the generation of the phone's Public Key
10 Certificate, its signing by the CA, and the certificate and CA's public key transference into the phone are deemed to be secure.

Also at the factory one or more License Certificates are issued (step 104). The factory sends a request to the CA server 15 (or the software server 17 under the root authority of the CA server 15) to sign a License Certificate (step 105). The
15 factory provides the CA information on which software licenses or products the phone is supposed to have along with the phone's serial number. The License Certificate includes the following information: (i) the CA's identification (the issuer); (ii) the serial number of the phone (the subject); (iii) a list of software products the phone is licensed to run; and (iv) a signed (encrypted with CA's private
20 key) digest (software hash) of the aforementioned components. The license certificate is installed in the phone at step 106.

The License Certificate may contain multiple licenses in one certificate, or there may be multiple License Certificates with one license per certificate. Both methods are allowed. The CA itself will retain a copy of the phone's License
25 Certificate(s).

Now, the phone enters the software programming phase. The phone msut contains various amounts of software - some base version plus some (optional) additional features, depending on what was ordered. The factory must install the correct software package(s) into the phone. The software packages include the
30 software itself plus a Product Certificate (or more generally a content item

certificate). The Software Server 17 generates a Product Certificate (step 110) for each software product under the same root authority as the CA. Both the software and Product Certificate are stored on the Software Server 17. The Software Server 17 is responsible for managing the software products and making them available for download. The software package and its certificates (i.e. digitally signed software) is installed in step 112.

The purpose of the certificate is to bind (i.e associate) the software product to a particular name (e.g. software product name and major version number). This association may be in the form of a look-up list of product names associated with the certificate of a product name and a predefined rule identifying permitted new product names (e.g. Browser version 1.x permits all future versions of Browser between version 1.0 and version 2.0). The certificate contains the name of the software along with a hash of the software product. Anyone wishing to validate the integrity of the software can hash the software and compare it to the one found in the Product Certificate. The certificate is signed by the Software Server. The Software Server itself has a Public Key Certificate signed by the CA, so a line of trust is maintained.

The Product Certificate includes the following information: (i) the Software Server's identification (the issuer); (ii) the software products name (the subject); (iii) a hash of the software product; and (iv) a signed (encrypted with Software Server's private key) digest of the above components.

The Software Server 17 retains a copy of the Product Certificates. It should be noted that the CA 16 may also perform the function of the Software Server 17, in which case the CA will be responsible for all three types of certificates.

The phone leaves the factory installed with: (i) the CA's Public Key Certificate; (ii) the phone's Public Key Certificate; (iii) one or more License Certificates; and (iv) one or more Product Certificates.

A series of steps takes place every time a user turns on the phone. First, the phone's boot software validates all of its Product Certificates (step 130). That is, a hash is computed for each software product in the phone.and compared against the hash stored in the certificate. Also, a line of trust to the CA must be established.

9

Since the Product Certificate was signed by a Software Server, not the CA, the phone will obtain the Software Server's Public Key Certificate from the CA (this should only occur one time after which the phone will store the Software Server's Public Key Certificate in memory). Next, the phone's boot software validates (step 135) all

5   of its License Certificates. That it is, a comparison between the phone's unalterable serial number and the serial number stored in the License Certificate(s) associated with the products is made. If they match then the phone is allowed to operate the software products identified in the License Certificate. The software products identified in this certificate must match the software products name field in the

10   Product Certificates. In both steps, the phone's boot software compares the digital signature of the certificates with the CA's Public Key Certificate (which was installed in the factory) to ensure that forged certificates were not installed.

In the event that a user wants to modify the phone, such as enabling an option or purchasing a new feature (see Examples below), a new License Certificate is

15   obtained along with the software product itself plus its Product Certificate. The following steps take place. First, the user purchases the feature through the Web Server 16. Whether by phone or Web access, the user submits the necessary information to the Web Server 16, including name, address, credit card number, the phone's serial number, and desired product to purchase (step 16). The Web Server

20   16 verifies the information and creates an order ticket which is also given to the customer. Assuming the customers credit has been validated, the Web Server 16 sends the phone's serial number along with the name of the software product purchased, to the CA server 15 to obtain a new License Certificate.
The License Certificate is made available to the phone to download (step 204). The

25   user may initiate a sequence to obtain it. The phone validates the new License Certificate. If the software product was installed in the factory but not enabled (no license certificate), it will now be enabled (step 220). If the software product is not found in the phone, it will send a request to the Software Server to obtain it (step 226).

10

As an optional step, the Software Server 17 may be configured to send software products encrypted and only to authenticated users, in order to prevent overloading of the wireless network and to prevent unauthorized users from obtaining the software code (despite the fact that the phone cannot run the software
5   anyway without a valid License Certificate). This is done by establishing a WTLS connection between the Software Server 17 and the phone 11 via the WAP proxy server 18. Each party has a Public Key Certificate signed by a common CA, so they trust each other's certificates. Using a key exchange algorithm, a secret key is derived and used for encrypting the software product and Product Certificate. The
10   Software Server then sends the software product and Product Certificate over the air to the phone, the phone validates the Product Certificate and the purchase is complete.

Note that in this model, if the download is interrupted or the software is corrupted, the user can retry the download any number of times.
15   In the event that the phone has to be brought in to a repair shop, there are a number of features in the secure electronic commerce system available to make updates or modifications to the phone a painless one. For example, if for some reason a different phone is issued to the user, the repair shop could transfer all of the contents of the existing phone (software and Product Certificates) into the new one.
20   The new phone will not be able to run the software until a new set of License Certificates is generated for that phone's serial number. The repair shop requests new License Certificates from the CA using the repair shop's Public Key Certificate as proof to the CA that it is empowered to do so. The CA has on record the License Certificates for the existing phone. New License Certificates are issued for the new
25   phone, and the existing phone's License Certificates are put on a certificate revocation list. If for some reason the repair shop needed to copy software into the new phone and was unable to copy it from the existing phone, the software (and Product Certificate) could still be downloaded from the Software Server as described previously.

By implementing the secure electronic commerce system, new features, updated software, and software patches can be delivered to the phone in a timely efficient manner for the customer. The customer benefits from the ease of performing the tasks, and the almost immediate cycle time to achieve it.

5 Furthermore, the security features built into the system will reduce incidents of theft of service or cloning.

The following examples help clarify what potential solutions are available in a secure electronic commerce environment for some real world situations.

10 Example 1 - Acquiring an application not currently in the phone

A user is travelling overseas and wants to have access to a voice activated German/English translator on their phone. The user can purchase the German/English translator software product from the manufacturer or retailer. The user will download the application into the phone and the German/English translator

15 is operated locally on the phone, rather than through the service provider's infrastructure. This is more cost effective if the user plans to use the feature on a regular basis. The user feels a sense of ownership. As long as the user keeps the phone, he/she owns the software. The software operates locally in the phone. The user does not access the feature over the air, thereby eliminating any potential out-of-

20 service conditions, bandwidth or throughput issues, or unexpected infrastructure downtime. The user pays the manufacturer or the retailer for the feature, rather than the service provider.

Example 2 - Enhanced phone feature

25 A user wants to be able to use a new Web browser now available for the phone, either by downloading the software (if the phone did not contain the software when purchased) or by enabling access rights to the feature already stored within the phone. The user connects the web server 16 (or 1-800 number), follows instructions to purchase additional options for the phone, and waits a short time for the software to be downloaded,

· 30 or enabled, with the new Web browser capability. The user gains instant satisfaction by

accessing the feature minutes after the purchase is made. The cost of the feature is lower than it would otherwise be because the overhead to bring the feature to the user via electronic download is low. Because the transaction is authenticated by the certificate authority via the CA server 15. theft of service is virtually eliminated.

5

Example 3 - Software patch update

A software patch is issued to the field to be installed in an existing phones (e.g. under warranty for no charge). The user is instructed how to enable the phone to begin a download containing the updated software. Another option is that the service provider can

10   automatically update phones while the phone is in service, without the user aware of the upgrade. The user does not need to physically return the unit to a service shop. The user's phone is updated in a matter of minutes, rather than days spent in a service shop. An instant electronic record of the software download is retained in the system 10, rather than relying on field service reports. Certain upgrades can be done automatically without the user's

15   consent, thereby eliminating any service interruptions. The cost is minimal because no service shop is involved in the procedure.

Example 4 - Metered service

A user wants to access an audio book in his/her car during the commute

20   to/from work. The user can purchase an audio book from a service provider. Access may be gained by means of a secure data service connection which allows the metered service (either per book or per minute). Among other options, two-way communications allow the user to suspend/resume the transmission. This is a new type of service not achievable without secure electronic commerce.

25

Thus a wireless electronic commerce system has been described having a wireless gateway 18 to a wireless network 19 with which a wireless client device 11 having a unique client identifier is capable of communicating. At least one server has been described coupleable to the wireless gateway, delivering content items to

30   the wireless device and maintaining digital content certificates for content items and

13

digital license certificates for licenses for the content items. In the preferred embodiment the server 17 delivers the content and the CA server 15 maintains the digital license certificates. The at least one server maintains, for each wireless client associated with the system, a record of licenses for that client and a record of content

5   items associated with each license. In other words, the CA server 15 maintains a database or list correlating wireless client IDs with licenses (or license certificates) for each client ID and content items (e.g. software products) associated with the licenses.

It has been described that the wireless client is able to request digital license

10   certificate verification for a new content item when the new content item is associated with an existing digital license certificate that is associated with the client identifier. Content of a first wireless client with a first identifier is preferably able to be replicated in a second wireless client with a second identifier by reloading the content to the second wireless client; replacing, in the at least one server, a first

15   association between the first identifier and corresponding records of first client licenses and first client content items, with a new association between the second identifier and the corresponding records of first client licenses and first client content items; and verifying, for the second client, the first client licenses and first client content items, whereby the second client is able to assume the functionality of the

20   first client.

Also described is a method of operating a wireless electronic commerce system comprising: maintaining at at least one server, digital content certificates for content items and digital license certificates for licenses associated with the content items; maintaining at the at least one server, for each wireless client associated with

25   the system, a record of licenses for that client and a record of content items associated with each license; establishing communication between the at least one server and a wireless client device via a wireless gateway; delivering a content item to the wireless device having a unique identifier within the system; verifying the content item with the at least one server; verifying a license associated with the

14

content item; and enabling the content item at the wireless client when the content item and license are verified.

The license for the content item is preferably verified when a name for the content item is pre-associated with a digital license certificate associated with the

5 unique identifier for the wireless device. Alternatively the name for the content item satisfies a predefined rule of a digital license certificate associated with the unique identifier for the wireless device, for example it falls within a range of permitted version numbers identifying it as an upgrade of a content item pre-associated with the digital license certificate.

10 The secure electronic commerce system described offers a solution to enabling software sales over wireless networks. The system is a robust, efficient, and user-friendly method to provide e-commerce services for customers.

The system has been described with a Wireless Application Protocol (WAP) server or gateway 18, but it will be understood that any wireless network gateway

15 can be used, WAP being merely a convenient protocol. Alternative aspects of the system are now described, also in the context of a WAP protocol and it will be understood that other protocols can be used.

Further details of the WAP server and WAP layers of the secure wireless electronic commerce system are now described. A set of WAP protocols in

20 transport, security, transaction, session and application layers are described in the document "Wireless Application Protocol Architecture Specification" [WAPARCH], WAP Forum, 30-April-1998. WAP security functionality includes the Wireless Transport Layer Security [WAPWTLS] WAP Forum, 30-April-1998 and application level security, accessible using the Wireless Markup Language Script [WMLScript].

25 The security provided in WAP can be of various levels. In the simplest case anonymous key exchange is used for creation of an encrypted channel between server and client; in the next level a server provides a certificate mapping back to an entity trusted by the client; and finally the client itself may possess a private key and public key certificate enabling it to identify itself to other entities in the network. The

30 infrastructure and procedures required to enable the trust relationships needed for

authentication of servers and clients are described in greater detail here. The term "server" used here is not limited to a dedicated WAP gateway but may include third parties and content/service providers using the WAP protocols. The specifications for the aforementioned and other WAP protocol layers are found at URL:

5   http://www.wapforum.org/.

In addition to the above-mentioned documents, reference can be made to: "Wireless Control Message Protocol Specification", [WAPWCMP] WAP Forum, 30-April-1998; WAP Identity Module Specification [WIM], WAP Forum, 12 March 1999; Digital Certificates for Mobile, Account Based, and High Transaction Volume

10   Financial Systems [X968], 1 March 1999 ANSI draft; "Standard Specifications For Public Key Cryptography", IEEE P1363 / D1a (Draft Version 1a) [P1363], February 1998. URL: http://grouper.ieee.org/groups/1363/; PKCS #1: RSA Encryption Standard", version 1.5 [PKCS1], RSA Laboratories, November 1993; PKCS #15: and Cryptographic Token Information Standard" [PKCS15], working draft version

15   1.0, RSA Laboratories, November 1998.

To describe further aspects of the electronic commerce system, the following are now described: the security domains; the attributes to be distributed/protected in the system; attribute ownership assigned to domains (note some attributes are owned by more than one domain); and the architecture for the enrollment and authentication

20   of domain members and assignment of attribute.

A "domain", or "security domain", is a public key infrastructure under the control of a single authority and using a defined internal naming scheme, algorithms, and policies. Domain authority flows for a domain root certification authority having a globally unique name. This allows domains to generate agreements and hook

25   together forming a global PKI. An entity that has been enrolled in a domain by the certifying of the public key that the entity owns within the domain is a "domain member". The following are the possible WAP domains, some or all of which will be referred to: manufacturer(s); network; operator(s); wireless service provider(s); content/services providers (e.g., banking domain); trusted third party domains (e.g.,

an independent certification agent or authority); device owner (fleet operator domain); and device user (personal domain).

An "attribute" is either a characteristic (which can be considered to be a name) or a right (i.e. a permission, for example a permission to access a purchased
5   service). Examples of attributes, are owned objects (e.g. directories & files, hardware and & interfaces) and owned rights/permissions (e.g. make call; establish network connection; send SMS message; read/write/update files & directories; configure device hardware; access network management station.

In order to implement this security infrastructure, the WAP Public Key
10 system 10 enrolls and authenticates WAP domain members and distribute attributes. Note that the word "distribute" includes "distribute to purchaser"; i.e., subscribers may be purchasing attributes such as access to content or services.

The WAP PKI architecture consists of autonomous security domains tied together by cross-certification. Such cross-certification is a part of service roaming
15 agreements between service providers and system operators. Cross certification is the process by which two domain root CA's issue one another cross-certificates; thereby authorizing one another's root certificates (keys). Cross-certificates generally contain the address of one or more inter-domain validation servers and may also contain other information related to the cross-certification agreements. For the wireless
20 industry cross-certification can be similar to creation of roaming agreements. Within a security domain the algorithms, naming scheme, and policies of that domain are determined by the owner of the domain. During the cross-certification procedure, domains agree on inter-operability issues and configure validation servers to allow certificate validation to be performed.

25   Classes of WAP operation are: class 0: anonymous authentication only; class 1: server authentication only; and class 2: server and client authentication. Class 0 is not of concern here as it does not involve a PKI. Class 1 involves the authentication of servers to clients. These servers may be owned by the wireless service provider or may be third party servers offering their services in the network. By including these
30 third party servers in the WAP PKI the wireless service provider indicates a special

17

status or stamp of approval to these services. Class 2 operation allows a client (mobile subscriber) to enroll as a member in the domain and obtain benefits of being in such a domain. This may involve special agreements with third parties such as discounts or special services. Domain members may be issued small attribute

5   certificates, tied to their domain private key, that indicate purchased services or special rights being granted.

Attribute certificates are of two types: (i) purchased service or product certificates, which are like monthly subscriptions and do not require special revocation procedures; and (ii) system operations permissions, which are attributes

10   issued to allow users special system configuration rights. These latter may be used by wireless service provider personnel or issued to authorized subscribers.

Above, several domains have been identified. The usage of some of these domains is now described.

The device owner domain is a domain used to set up device users and user

15   profiles/privileges without wireless service provider involvement. This could be done by having the service provider give the device owner a service provider domain identity and attributes to modify their account configuration. Or the device owner could be made an attribute authority in the service provider domain. The device owner does not necessarily need his own domain, although in a large fleet where

20   device owner needs to issue certificates to employees allowing them certain rights it is preferable to have such a domain. The system allows for device owner domains, although they are not expected to be deployed initially as simpler means (using service provider domain) exist for the required functionality.

Manufacturer domain is used for device bootstrap, device OS code upgrades

25   & features.

Wireless service provider domain and/or network operator domain can be used for WAP gateway certification, content provider certification, subscriber feature distribution, subscriber identification (bind to account), WTA scripts, over air system modifications, distribution of certificates to employees to allow system

30   configuration.   Content/service provider domains can be used for security

18

conscious entities (e.g. banks) to run their own domains that cross-certify to operate with service provider domain or enroll wireless users directly.

Note that a user may be a member (have a key certified) in any domain. A domain is used to issue certificates to grant permissions to others in a system; permissions can be controlled on the device in a simpler manner.

Focus of further discussion herein is directed to the service provider, network operator, and manufacturer domains, with particular reference to FIG. 4.

FIG. 4 illustrates a CA 400 (implemented as a server). A certification authority is an entity that issues/updates/revokes public key bearing certificates in response to authenticated requests from legitimate registration authorities. The CA holds a private key used to sign domain member key bearing certificates. The CA is managed by a wireless service provider or network operator controlling and operating a wireless network via a wireless network controller 401 and generating bills for customers via billing computer 402.

A plurality of Attribute Authorities 404, 405 and 406 are shown (three are illustrated, but there may be many). An Attribute Authority is an entity that generates certificates assigning attributes to domain members. Examples might be a mobile telephone manufacturer 404, a book merchant 405 and a wireless software supplier 406.

The AAs can communicate with the end user (client) device 450 via a wireless gateway 420.

The client device 450 preferably (but not necessarily) has a Subscriber Identity Module (SIM) 452. This is a smart card in a wireless system holding subscriber identity and authentication information. The SIM card can also be used to run applications needing a secure environment. The client device preferably also has a WAP Identity Module (WIM) that provides an interface for service relating to the use of the WAP security layer as well as data storage services. The WIM uses PKCS15 for object formats. The WIM may be an interface layer to the SIM card 452, or it may be a SIM or other card with a native WIM interface on it, or a software token on the wireless device 450.

19

All items of FIG. 4 belong to a domain 500, which in this embodiment is a wireless network operator domain. The domain 500 may have a higher registration authority, that is an entity authorized to make requests to issue/revoke/update certificates to a CA or AA. The registration authority can be considered similar to an

5   account manager in function and is responsible for member enrolment and/or attribute assignments. Enrollment is the process by which a user public key is certified in a domain by the issuance of a domain certificate containing this key.

Server 400 is a validation server. A validation servers is a server that is configured to validate certificates for domain members. Domains that cross-certify

10   are expected to provide accessible validation servers that obtain and validate certificate chains. This service is important when there are domains with local naming schemes. Since these schemes may not be understood by an outside domain, it is necessary for the validation service to be provided. A validation server that is configured to communicate with one or more outside domains is an inter-domain

15   validation server. In addition validation servers may provide local domain validation for thin clients that are domain members but do not have the ability to obtain and validate a certificate chain on their own.

It is possible to have multiple wireless service provider domains stored in the system. If a customer switches providers in a system with a WIM identity card

20   having personalization and key information on it certain issues arise. If the user simply obtains another card from the new provider all the personalization information will be lost. It is therefore good practice, although not essential, that service provider specific information is separated from personalization information not dependent on the service provider. It is also preferable to provide a means for the

25   user to create a WIM software token to be used to initialize a new WIM card.

It is advantageous for certain businesses wishing to sell services or content to mobile subscribers to have their own security domain. This may be required for certain financial services for risk management reasons. The keys and applications for these domains must be separated from other domains in such a way that the

30   owner is confident that no tampering is possible. Although it is possible to store

certificates and keys from any domain in the WIM, this separation can be implemented in various ways that need not be described. In addition to stored object separation the device must insure that domain applications cannot be tampered with.

Any domain member may become an attribute authority. Wireless service
5   providers distribute system management attributes to merchants that they bring into their domain who can sell their attributes- i.e. sell a purchased service ticket (e.g. for new software as described above or for other content or services).

There are three types of payloads: compact payloads, organizational payloads of which WAP payloads are one type, and domain specific payloads that are valid
10   only in a local domain.

In order for merchants operating AA servers 404-406 to define simple attributes for the service/content they sell, it is necessary to have a method to indicate that a given attribute payload is a merchant payload and to indicate the particular merchant. Since the payloads are not expected to be understood by anyone but the
15   merchant the actual structure of the payload is not material. There are three ways that merchant attribute payloads may be identified: (i) if the merchant has an organizational identifier it can define its types under this identifier; (ii) merchant identifiers can be assigned under the WAP OID; (iii) domains can define and deploy a merchant ID scheme for their domain specific payloads.

20   Attribute certificates are preferably time-limited, i.e have an expiry date and be subject to periodic renewal. At any time when a certificate is verified, verification fails if an expiry time digitally embedded in the certificate has expired.

A mobile client checks the validity of a merchant server (404-406) with the network upon first use or periodically. The client (either the wireless device 450 or
25   the SIM 452 can be considered a client) contacts the validation server via the wireless gateway 420 for this purpose. In addition the wireless service provider may post a web site listing the status of domain merchants. Such a site could also indicate if the merchant is no longer a trusted domain member; i.e., if their certificate has been revoked for some reason.

The steps by which a merchant (i.e. an AA) or other network element having the apacity of an AA delivers content to a client and receives payment for that content is now described with reference to FIG. 5.

Initially, a client (450 or 452) establishes connection in step 510 with an AA server 404 via the wireless gateway 420. The AA delivers a digital certificate to the client in step 515. The client verifies the AA certificate in step 520. This is achieved at the client in the same manner as other certificate verification already described and is achievable because the client already has installed the public key certificate of the CA 400. It uses this public key certificate to verify the AA. The reason for this verification is because the client wishes to have confirmation that the AA is trusted by the wireless service provider. This will give the user confidence that the content to be delivered by the AA will operate when delivered to the wireless device 450, that it will not cause disruption, that the fee to be paid is as advertized, that upgrades will be available, etc. There are many reasons why the user may wish to ensure that the AA is certified by the wireless service provider.

Next, an exchange occurs between the client and the AA to deliver payment to the AA for the content that the client is about to receive. This transaction can take one of several forms. The AA informs the client what the fee is for the content to be received and the client, if the user so chooses, authorizes payment of that fee. For example, the client can provide credit card details (step 535) and the AA server can establish a connection with a credit card server to execute a transaction (step 530). Alternatively, the client can deliver electronic cash to the AA server (step 535 (which need not be described). In a more preferred alternative arrangement, the client delivers a certificate to the AA that is certified within the wireless service provider domain 500, i.e. is certified by the CA 400 and has the public key certificate of the CA 400 (step 540). The AA server verifies this certificate in step 545 (using the root public key certificate that it already has stored at the AA server) and the AA is ready to deliver the content item (attribute) to the client. Upon delivery of the content item to the client (step 550) the AA instructs the CA to bill the customer for the predetermined fee (step 555) and the CA 400 instructs the billing computer 401 to

add the fee to the customer's bill (step 560). Meanwhile (step 570) the content item is enabled on the client.

Enabling of the content item can take many forms, for example executing a software application or an upgrade or patch to a software application, or displaying a

5   newspaper, or delivering a stock quote service, or opening wireless web access to a streaming video service or music service, or delivering an electronic airline ticket or a ticket to a concert, or many other examples. In effect, the various AAs 404, 405, 406 all provide a virtual wireless shopping mall with a common billing mechanism, which is the billing mechanism of the wireless service provider.

10   If steps 535 or 525 are executed, it is not strictly necessary for the AA to perform online certificate validation of the client's certificate (steps 540 and 545), but is preferable to do so anyway. As an alternative to the step of verifying the AA certificate (step 520) the client can just check the last posted AA list (or AA revocation list). In addition the domain provides a service that notifies merchants

15   when a client certificate is revoked, so as an alternative to step 545, the AA can check this list. Of course, if the client is charged by electronic cash or credit card, steps 555 and 560 are omitted.

Although several domains may be useful, it is not necessary to have users become members of these domains by obtaining a user key. In the case of a phone,

20   as already described, the manufacturer can enroll users if direct sales to a user of device feature upgrades are intended. This could, however, also be done through distribution through the service provider domain or assignment to device identifiers. Managing user keys may be less preferable in the manufacturer domain. This domain can preferably be used to authenticate features and upgrade scripts from the

25   manufacturer.

If the network operator runs a security domain, client keys may be required, but only for clients that are to be authorized to perform network operations from the mobile device (i.e., network operator employees). General client authentication to the network operator is not strictly necessary.

The case of the wireless service provider assigning keys to users is of particular interest. The client keys are distributed in the WIM card when service is purchased. The client key in the wireless service provider domain allows a member of this domain to assert an identity that is bound to the account with the provider.

5   The service provider or its authorized third parties may then sell content/services in the domain. The client key also allows certain clients (say, service provider employees) to use the system to identify themselves to the network as having network operations permissions.

For service and content providers other than the wireless provider that require

10   separate security domains client keys are preferably issued and stored in the WIM. Domains are permitted to specify any naming scheme consistent with their network and are responsible for assuring that this scheme is internally consistent. A domain's internal directory service must be configured to resolve local domain names. Names may be of multiple type including email addresses, IP addresses, DNS names, and

15   account numbers. The business deploying (or contracting for deployment of) a domain may configure the naming mechanism to suit their business and system needs.

The AAs 404, 405 and 406 can communicate between each other via links 408 and 409 to exchange electronic vouchers. For example, AA 404 can advertise to

20   its clients that purchase of its services earns for the client a credit for the services offered by AA 405. When a cleint purchases a ontent item from AA 404, AA 404 generates an automatic voucher that it delivers to AA 405, identifying the client by ID and the credit to be attributed to that client. When the client establishes a connection to AA 405, the client is informed of the discount from the fee of AA 405

25   that this particular client has earned. If the client purchases a service from AA 405, the latter can charge AA 404 for the value of the discount voucher or a portion thereof. There are many variations on this scheme that will be readily apparent to one of ordinary skill in the art. For example, points can be accumulated by the billing computer at the CA 400 that can be used at any of the AAs 404-406.

30   Alternatively, the voucher can be transferred to the client 450 or 452 instead of

24

between the AAs so that the client can deliver the voucher to the next AA in the virtual wireless mall. This latter scheme is particularly simple to implement using the already describes public key certificate common to all the members of the domain 500, because any AA in the domain can readily verify the authentiity of the

5   voucher.

Further miscellaneous details of the overall secure wireless electronic commerce system are now given for completeness.

Directories are organized as: domain authority name->fully qualified local descriptive name->key hash, certificate hash, or key ID or domain authority name-

10   >key hash, certificate hash. Within a domain the domain authority name is implicit. A fully qualified local name is a local name that is unique within the domain; in some cases this is a combination of the issuer and subject names in a certificate (subject relative to issuer). The use of the certificate or key hash alone (no descriptive name part) for entity names is less preferable due to the difficulties it

15   creates in directory lookup and certificate chain validation.

An issuer below root has a name consisting of either a certificate hash and an optional descriptive name, a key hash and an optional descriptive name, or an integer key identifier and a descriptive name. Use of the integer key identifier and descriptive name allows for shorter and more human readable names.

20   The validator has means to obtain the necessary certificate path when a transaction requires that a certificate chain be processed. In many cases the end entity certificate itself will not be sent, only a name or names that allow the validator to obtain any required certificates. Within a domain this can be made simple by using a deterministic path naming scheme that allows the certificate validation path

25   to be obtained directly from the (issuer, subject) pair. If the naming scheme does not do this internal to a certificate then a means external to the certificate must be provided to obtain the proper path. For validation between cross-certified domains it is recommended that a domain provide a secure validation service for its certificates. If a domain is to validate certificates from other domains internally then it must

30   understand the naming schemes and algorithms used in the other domains.

In certain cases a CA may have more than one valid certificate listed at a given time. This could happen during a scheduled re-key of the CA. This creates a possible problem when trying to follow a certificate chain as at some point the chain allows multiple possibilities. There are several methods for dealing with this: (i) trial and error, which is inefficient due to the need to check multiple signatures for a match; (ii) use of a name type containing a key or certificate hash for CA's and AA's. This resolves ambiguity but makes names larger; (iii) use a key identifier with a descriptive name . This latter is the preferred method.

Given that some devices may not be capable of processing certificate chains for intra-domain validation, a validation service is defined in X9.68. This service is realized by providing validation servers in a domain. The addresses of these may be indicated as payloads in CA certificates or configured in some other manner. The client of the service must be able to verify the signature on the response so it must have the validation server certificate or be able to verify this certificate. A thin client receives a certificate that it wishes to validate along with an indication of the domain authority of the certificate; the domain is its own. The client sends a validation request to a validation server. The server sends back a signed validation response.

For inter-domain validation, domains make certain services available to other domains. A cross-certificate indicates where these services may be obtained by providing an address for servers offering such services. The validation service operates between a validation client, which may be an intra-domain validation server, and an inter-domain validation server. An inter-domain validation server is expected to be able to contact and verify the authenticity (signature) of a response from another domain's validation server(s). Note that this implies that inter-domain validation servers must be capable of using the algorithms from the other domain. Inter-domain validation servers are members of multiple domains and therefore are able to verify signatures of other domains. A thin client receives a certificate that it wishes to validate along with the domain authority of the certificate; the certificate domain is not its own. The client sends a validation request to a domain validation server. Note these servers can be indicated in the root certificate as payloads or

26

stored elsewhere. The validation server notes that the domain is external. It determines if a cross-certificate with the indicated domain exists. If not a validation failure response is returned to the client. (Note that this third step can be skipped if the client is aware of the address of an inter-domain validation server). If a cross-certificate exists and the server is an inter-domain validation server it handles the request itself; otherwise it signs and sends a validation request to an inter-domain validation server listed in the cross certificate. The inter-domain validation server authenticates the request and either verifies the certificate itself or passes the request to an internal validation server in the other domain. The result is signed and returned to the validation server the client originally contacted. The validation server authenticates the response, signs it itself, and returns it to the client.

The validation service allows an entity from one domain to request that a certificate from another domain be authenticated. A reply of invalid is required to be returned unless the server can ascertain that the certificate is currently valid. A reason for the failure is preferably provided.

Each domain selects the algorithms to be used internally for digital signatures, data encipherment, key encipherment, and key agreement. In addition the maximum key size that can be used inside the domain is given by the domain root CA key size. Domain members must have the cryptographic software/hardware implementing the domain algorithms with the maximum key size. In addition a domain member must have a securely loaded and stored domain root CA certificate or a condensed form of the domain root CA certificate information.

A domain is defined so as to fix the algorithms used within for efficiency reasons. As a domain selects RSA with a given root key size the algorithm and key size are known for every client in that domain. This makes the impact of supporting another algorithm for a mobile client explicit- every new domain the client joins is potentially a new algorithm. In fact, for security reasons, some domains may not even allow another domains code to be used even if the algorithm is the same.

A domain root CA indicates the algorithms, internal naming scheme, and policies in effect in the domain. Policies include such information on what guarantee

the domain makes of member identity binding to account and what procedures and guarantees are made for third parties issuing attribute certificates in the domain. In addition specific policies for each cross-certification agreement are maintained.

5   The process of cross-certification is one in which two autonomous security domains grant formal recognition to one another. This is done digitally by each domain creating and signing a cross-certificate object containing the other domains root certificate (or its hash). In addition the addresses of inter-domain validation servers and indications of contractual agreements may be contained.

10   For service provider domains in systems with SIM or WIM smart cards that are personalized at the time of service subscription, member enrollment comprises storing the member certificate and key on the WIM card.

For systems not having a smart card, the keys and certificate are stored in a WIM software token. Member keys are protected by passphrase information. This information is concatenated with a stored secret value for the device and run through 15 a secure hash in order to generate the encryption/decryption key for use in protecting the user private key.

Member certificates are also kept with the member's account and entered into the service provider member directory. In some systems the actual member certificate may not be stored on the WIM itself but maintained in the system only. For this 20 usage the member certificate can be used as a secure container for account information and a client need only to present his identity to the system; the system obtains the required certificate. For domains other than the service provider the enrollment process requires that a secure manner to store the keys in the WIM be defined and that each domain is assured of information

25   System bootstrap involves the loading of the domain root certificates and client keys. Note that in addition to a client signature key, keys to be used for data encipherment, key encipherment, and key agreement can also be loaded. Signature keys for clients must be used only for signatures. Keys for the other purposes are also loaded. Initially the manufacturer domain root certificate is loaded into the 30 mobile device. This certificate is used to enable secure loading of other domain root

certificates if necessary. In systems not having a secure service provider provisioning scheme in place, the manufacturers provide certificates to service providers giving the service provider a provisioning attribute. This attribute allows a service provider to install their root certificate in the phone.

5   It is necessary to securely load and store domain certificates. Initially the device manufacturer certificate is loaded into the device as indicated above. Next service provider and network operator certificates are loaded. Once valid service provider and network operator certificates are loaded these domains gain control of attributes their domains own. Manufacturer domain loses control of any attributes it
10   does not own in a provisioned device.

For systems with SIM cards, the wireless service provider root certificate and client key and certificate are distributed on the card before it is issued to the subscriber. The means used to generate and bind the client key insure that only one binding is possible for a card and that signature keys cannot be determined by the
15   service provider or their employees. The personalization process binds the public key (and hence the private key) for a card to an individual account.

For systems without identity cards, the service provider and network operator certificates are loaded using the manufacturer root certificate to secure the loading process. The manufacturer issues certificates to service providers allowing them to
20   sign key loading scripts. The device must insure that only a properly authenticated request be used to load a domain root certificate.

During a planned re-key, each CA or AA simply re-issues certificates. A device must be able to accept a certificate change order for a certificate signed by the owner of that certificate.

25   When a CA or AA key other than root is compromised, messages from root can instruct the WIM to replace the key with a new key. Using root for this purpose means lower level CA's need not have their own disaster recovery keys, only root requires a key for this purpose.

When a root key is compromised it is desirable to have procedures in place
30   allowing recovery without re-enrollment of all domain members. For this reason

29

each domain preferably has a disaster recovery public key for a domain securely

stored in the WIM along with the domain root public key. The private disaster

recovery key must be kept in a separate system that is not connected to any network

unless disaster recovery is underway. It is desirable that the location for this key be

5   physically separate from the domain root key. Disaster recovery messages are

messages instructing the WIM to automatically replace a root key. It is required that

both the current root key and the disaster recovery key sign the root public key

change message. Receipt of a request for which one signature checks but the other is

invalid must cause the WIM to be disabled. It is also required that a message

10   disabling the SIM/WIM card entirely, signed by the disaster recovery key, be

supported. In summary, the disaster recovery process is:

message to change root signed by current root key and disaster key; (ii) message to

fully disable WIM may be signed by either root or disaster recovery key; and (iii)

receipt of a partially invalid request must cause WIM to be disabled.

15   A member device has keys associated with it that may be used for

transactions or authentication. These keys are generally protected by a PIN code and

some "maximum number of tries" deactivation protocol. It is desirable that when a

device is reported stolen, and the report itself has been authenticated in some manner,

the system be able to cause a card to clear keys remotely if someone attempts to use

20   the stolen device.

Thus a method of conducting transactions in a wireless electronic commerce

system has been described, where the system comprises a wireless network operator

certification authority having a root public key certificate and at least one attribute

authority having a digital certificate that is dependent from the root public key

25   certificate, where the attribute authority is accessible by a wireless client device via a

wireless network. According to the method described, a wireless communication is

established between the wireless client device (450 or 452) and the attribute authority

(404, 405 or 405). The digital certificate is delivered from the attribute authority to

the wireless device, the attribute authority is verified to the wireless client device

30   using the digital certificate and the root public key certificate pre-loaded in the

30

wireless client device under authority of the wireless network operator. An attribute is delivered to the wireless client device over the wireless network and ultimately enabled at the wireless client device.

Payment for the attribute may be transacted by delivering a second digital
5 certificate from the wireless client device to the attribute authority and verifying the second digital certificate using the root public key certificate from the certification authority. An instruction is preferably transferred from the attribute authority to a billing computer of the wireless network operator to add an item to a wireless network operator bill for the wireless client device.

10 The second digital certificate may be pre-loaded into the subscriber identity module by the wireless network operator or pre-loaded into a wireless communicator under authority of the wireless network operator.

Also described is a method of conducting transactions in a wireless electronic commerce system comprising a wireless network operator certification authority
15 having a root public key certificate and at least first and second attribute authorities, having respective first and second digital certificates that are dependent from the root public key certificate, where the attribute authorities are accessible by a wireless client device via a wireless network. The method includes establishing a wireless communication between the wireless client device and the first attribute authority;
20 delivering a first attribute to the wireless client device over the wireless network; generating an electronic voucher verifiable by the second attribute authority; establishing a wireless communication between the wireless client device and the second attribute authority; requesting a second attribute from the second attribute authority; identifying the electronic voucher at the second attribute authority;
25 and delivering the second attribute from the second attribute authority to the wireless device. The step of generating an electronic voucher verifiable by the second attribute authority may include delivering the electronic voucher from the first attribute authority to the second attribute authority via a connection therebetween or may include delivering the electronic voucher from the first attribute authority to the
30 second attribute authority via the wireless client.

31

Also described is a wireless electronic comm ːce system comprising: a wireless network operator certification authority server having a root public key certificate; at least one attribute authority server coupleable to the wireless network operator certification authority server, having a digital certificate that is dependent

5   from the root public key certificate;   a wireless client device having pre-loaded therein the root public key certificate; a wireless network coupling the wireless client device to the at least one attribute authority server; verification means in the wireless client device for verifying the digital certificate to the wireless client device using the root public key certificate pre-loaded in the wireless client device; means (e.g. server

10   18 or gateway 420) associated with the attribute authority server for sending and means (e.g. a radio receiver in the wireless device 450) for receiving an attribute over the wireless network; and means for enabling the attribute at the wireless client device.
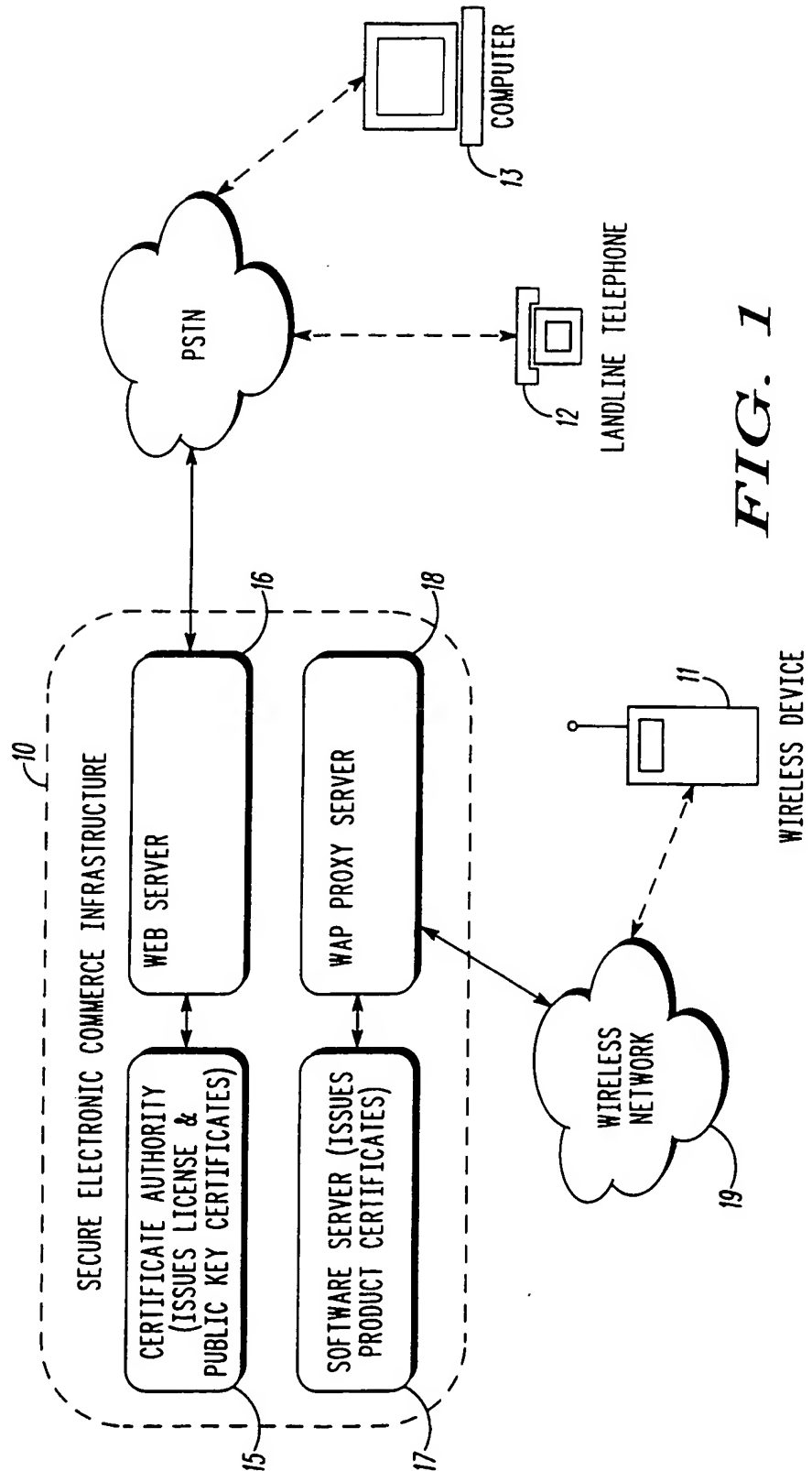
15

1.   A method of conducting transactions in a wireless electronic commerce system comprising a wireless network operator certification authority having a root public key certificate and at least one attribute authority having a digital certificate that is dependent from the root public key certificate, where the attribute authority is

5   accessible by a wireless client device via a wireless network, the method comprising:

establishing a wireless communication between the wireless client device and the attribute authority;

delivering the digital certificate from the attribute authority to the wireless device;

10   verifying the attribute authority to the wireless client device using the digital certificate and the root public key certificate pre-loaded in the wireless client device under authority of the wireless network operator;

delivering an attribute to the wireless client device over the wireless network; and

15   enabling the wireless attribute at the wireless client device.

2.   The method of claim 1, further comprising the step of executing a transaction whereby the wireless client device authorizes payment for the attribute from the attribute authority.

20

3.   The method of claim 2, wherein the step of executing a transaction comprises delivering a second digital certificate from the wireless client device to the attribute authority and verifying the second digital certificate using the root public key certificate from the certification authority.

25

4.   The method of claim 3, further comprising transferring from the attribute authority to a billing computer of the wireless network operator an instruction to add an item to a wireless network operator bill for the wireless client device.

5.   The method of claim 3, wherein the wireless client device has a subscriber identity module and the second digital certificate is pre-loaded into the subscriber identity module by the wireless network operator.

5   6.   The method of claim 3, wherein the wireless client device is a wireless communicator and the second digital certificate is pre-loaded into the wireless communicator under authority of the wireless network operator.
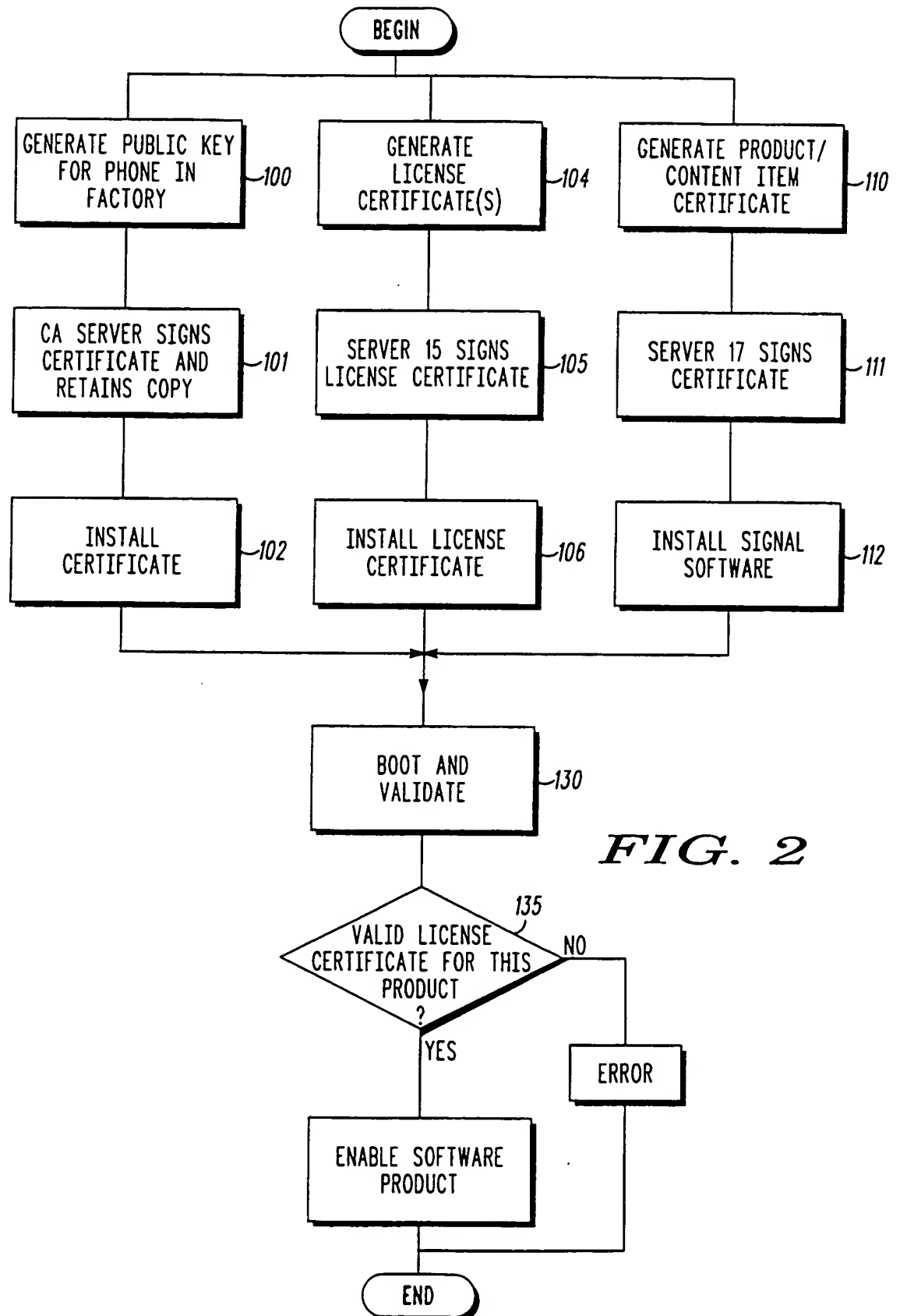
7.   A method of conducting transactions in a wireless electronic commerce
10   system comprising a wireless network operator certification authority having a root public key certificate and at least first and second attribute authorities, having respective first and second digital certificates that are dependent from the root public key certificate, where the attribute authorities are accessible by a wireless client device via a wireless network, the method comprising:

15   establishing a wireless communication between the wireless client device and the first attribute authority;

            delivering a first attribute to the wireless client device over the wireless network;

            generating an electronic voucher verifiable by the second attribute authority;

20   establishing a wireless communication between the wireless client device and the second attribute authority;

            requesting a second attribute from the second attribute authority;

            identifying the electronic voucher at the second attribute authority; and

            delivering the second attribute from the second attribute authority to the

25   wireless device.

8.   The method of claim 7, wherein the step of generating an electronic voucher verifiable by the second attribute authority includes delivering the electronic voucher from the first attribute authority to the second attribute authority via a connection

30   therebetween.

9.   The method of claim 8, wherein the electronic voucher identifies a wireless client for which the voucher is valid.

5   10.   The method of claim 7, wherein the step of generating an electronic voucher verifiable by the second attribute authority includes delivering the electronic voucher from the first attribute authority to the second attribute authority via the wireless client.

10   11.   A wireless electronic commerce system comprising:

a wireless network operator certification authority server having a root public key certificate;

at least one attribute authority server coupleable to the wireless network operator certification authority server, having a digital certificate that is dependent

15   from the root public key certificate;

a wireless client device having pre-loaded therein the root public key certificate;

a wireless network coupling the wireless client device to the at least one attribute authority server;

20   verification means in the wireless client device for verifying the digital certificate to the wireless client device using the root public key certificate pre-loaded in the wireless client device;

means associated with the attribute authority server for sending and means associated with the wireless client device for receiving an attribute over the wireless

25   network; and

means for enabling the attribute at the wireless client device.

FIG. 1

2/5

FIG. 2

PURCHASE FEATURE
THROUGH WEB
SERVER 16 — 200

SERVER 16 VERIFIES — 202

SEND ID AND PRODUCT
NAME TO SERVER 15
FOR NEW LICENSE
CERTIFICATE — 203

DOWNLOAD CERTIFICATE
TO PHONE — 204

(SOFTWARE
PRE-INSTALLED)

(SOFTWARE NOT
PRE-INSTALLED)

206 VALID
?

ENABLE SOFTWARE — 220

END

ERROR

208

SEND REQUEST TO
SERVER 16 AND DOWNLOAD
SOFTWARE

226

VALID
?

228

ENABLE SOFTWARE — 230

END

FIG. 3

FIG. 4

5/5

```
┌─────────────────────┐
│ CLIENT ESTABLISHES  │
│ WIRELESS CONNECTION │─510
│ TO AA VIA WIRELESS  │
│     GATEWAY         │
└─────────────────────┘
          │
          ▼
┌─────────────────────┐
│    AA DELIVERS      │
│   CERTIFICATE TO    │─515
│      CLIENT         │
└─────────────────────┘
          │
          ▼
┌─────────────────────┐
│  CLIENT VERFIES     │─520
│   CERTIFICATE       │
└─────────────────────┘
          │
          ▼
```

                                                                    525
```
┌─────────────────────┐   ┌─────────────────┐   ┌─────────────────────┐
│  CLIENT DELIVERS    │   │ CLIENT DELIVERS │   │  CLIENT PROVIDES    │
540─│   CERTIFICATE     │   │  E-CASH TO AA   │   │   CREDIT CARD       │
│      TO AA          │   └─────────────────┘   │  DETAILS TO AA      │
└─────────────────────┘          535            └─────────────────────┘
          │                                               │
          ▼                                     ┌─────────────────────┐
┌─────────────────────┐                         │ AA CONTACTS CREDIT  │
545─│   AA VERFIES      │                         │  CARD SERVER AND    │
│   CERTIFICATE       │                         │ VERFIES TRANSACTION │
└─────────────────────┘                         └─────────────────────┘
          │                                               530
          ▼
┌─────────────────────┐
│    AA DELIVERS      │
550─│ CONTENT ITEM (ATTRIBUTE)│
│    TO CLIENT        │
└─────────────────────┘              ┌─────────────────────┐
          │                          │  AA INSTRUCTS CA    │─555
          ▼                          │  TO BILL CUSTOMER   │
┌─────────────────────┐              └─────────────────────┘
│   CONTENT ITEM      │                        │
570─│   IS ENABLED      │                        ▼
│    ON CLIENT        │              ┌─────────────────────┐
└─────────────────────┘              │ CA BILLS CUSTOMER   │─560
                                     │  AND CREDITS AA     │
                                     └─────────────────────┘
```

FIG. 5